IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Richmond Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 3:19-CR-130-MHL
	)	
OKELLO T. CHATRIE,	)	
	)	
Defendant.	)	

GOVERNMENT'S RESPONSE IN OPPOSITION
TO DEFENDANT'S SUPPLEMENTAL MEMORANDUM
REGARDING MOTION FOR DISCOVERY OF SENSORVAULT DATA

The United States of America, by its undersigned attorneys, hereby submits this response to the defendant's supplemental briefing pursuant to the Court's Order entered on January 22, 2020. ECF No. 78.

The defendant's supplemental memorandum lays bare the boundless nature of his request to make Google, LLC ("Google") a member of the United States' prosecution team in this case. Although he argues that conclusion is required based on the particulars of this case, the circumstances he emphasizes would apply any time the government serves compulsory legal process on a technology company for a narrowly limited set of business records. Indeed, the defendant urges this Court to hold that Google is a member of the United States prosecution team for reasons that are not unique to this case: (1) Google advises on the contours of GeoFence warrants in turning over Google business records; (2) Virginia and federal statutes mandate that Google comply with such process; and (3) in complying with search warrants, Google searches its files for these pre-existing business records responsive to the search warrant.

But the defendant's proffered legal support leaves little doubt that his argument is novel.

No case law—much less binding precedent—supports the conclusion that a technology company's compliance with a search warrant turns them into a member of the United States' prosecution team. The Court should refuse to be the first court to so hold.

Most of the defendant's rationale for his theory focuses on Google's conduct in general—that is, not specific to *this* case. But no one would argue that Google's general conduct makes it an agent of the United States' prosecution team in any case, much less this one. The only rationale proffered by the defendant specific to this case is the correspondence between Google and the lead case agent—correspondence in which Google rebuffs the United States' requests at stage two of the search warrant. As explained in the United States' supplemental briefing, that back-and-forth did not turn Google into a member of the United States' prosecution team.

The defendant makes much of the Tenth Circuit's decision in *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), which itself applied "Fourth Amendment agency" principles stemming from the Supreme Court's decision in *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 614 (1989). That line of decisions, as several other district courts have observed, does not guide prosecution team analysis under *Brady v. Maryland*, 373 U.S. 83 (1963). Indeed, that line of decisions answers a question completely irrelevant here. Rather, that analysis answers whether a private actor's conduct during a warrantless search and seizure may be considered governmental conduct for purposes of the Fourth Amendment.

There is a meaningful difference between the private search doctrine and the scope of the prosecution team under *Brady*. The private search doctrine focuses on considerations that do not apply here: whether the government acquiesced in the search; and whether the search was intended to benefit the government or the private party. For one, the government did not acquiesce to Google—Google did no more than produce a set of information specified by a

search warrant and was resistant even in doing that. Responding to limited legal process does not make one a member of the prosecutorial team. And the benefit to the government, standing alone, cannot be part of the test for a prosecution team analysis, because every step taken to comply with a search warrant would benefit the United States. More importantly, Google's intent in providing a limited set of business records to the United States was compliance with a search warrant issued by a Virginia magistrate. For these reasons, the *Skinner* line of cases does not answer the prosecution team question at the center of the defendant's discovery motion. And, even if that test were somehow relevant, binding Fourth Circuit precedent suggests the answer would come out the other way in the context of a private actor like Google responding to a search warrant. *See United States v. Richardson*, 607 F.3d 357 (4th Cir. 2010) (rejecting argument that private technology company acted as agent of the government for purposes of a Fourth Amendment search).

The defendant's materiality arguments should also be rejected.[1] Materiality, by the defendant's measure, is satisfied where there is some conjecture of helpfulness. That is not enough. The Court should reject the defendant's attempt to lower the bar of materiality. And because suppression cannot be based on the privacy interests of other account holders, whatever the expert thinks about other individuals' Google information does not make it material here.

I. BACKGROUND

At the suppression hearing, the defendant's expert Spencer McInvaille gave equivocal

[1] The defendant spends portions of his supplemental briefing addressing requests aimed at law enforcement. Because the Court's order focuses on Google documents, the United States reiterates that there are no documents fitting those law enforcement focused requests. *See* ECF No. 28 at ¶¶ 8, 11. Nevertheless, the United States will advise the defendant of the lead case agent's rationale for culling from nineteen accounts to nine accounts as well as his reasoning for getting subscriber information for the final three accounts.

testimony regarding the information sought by the defendant. For example, when asked who might have information about the Wi-Fi access points for the location history information provided in stages 1 and 2 of the GeoFence warrant, the defendant's expert responded, "Google, *possibly*." Disc. Hr'g Tr. at 67 (emphasis added). In explaining that answer, the defendant's expert merely provided, "[w]ell they've got to have something to base[] the . . . location." *Id.* Then, when asked whether the access points would permit the parties to assess whether any points were outside the 150-meter radius relevant to stage 1 of the warrant, the expert demurred, "[i]t *could*." *Id.* at 68 (emphasis added). The expert's testimony remained elusive when addressing Google's algorithm—an algorithm he admitted he possibly might not comprehend or be able to manipulate. *Id.* at 72, 119.

The expert witness did not address other portions of the defendant's Motion. He gave no meaningful testimony regarding the parameters of Google's "Sensorvault data" (sought in Paragraph 4(a) through (e) of the Motion). Likewise, the defendant elicited no testimony or argument about the identity of Google analysts requested in Paragraph 5. When asked about Google's policies and procedures, the defendant's expert merely opined that he was "sure [Google] *would*" have such documents because "something guided them to provide a certain data or search a certain set of data." *Id.* at 31 (emphasis added). As the defendant's expert had to concede on cross-examination, his testimony on direct examination was an amalgam of "*could* be, *may* be, but *you don't know*." *Id.* at 120 (emphasis added). Lastly, the defendant's expert acknowledged that Google users voluntarily disclosed their location information and were appraised of the storage of this location information after the setup. *Id.* at 107.

II. ARGUMENT

A. Both parties agree that "government" under Rule 16 should be informed by Brady prosecution team precedent.

The defendant argues that "Google is part of the 'government' under Rule 16 for the same reason it is part of the 'prosecution team' under *Brady*." Def.'s Supp. Br. at 28, ECF No. 87. Although the defendant advances the wrong conclusion on Google's role as a member of the prosecution team in this case, the United States agrees that, as a practical matter, the best path to assessing the reach of "government" under Rule 16 in this case is to look to the *Brady* line of case law setting the scope of the "prosecution team." Through that lens, even the defendant's cited authority points the Court to the conclusion that, on these facts, Google is not a member of the prosecution team.

1. The Tenth Circuit's decision in *Ackerman* does not apply to this case.

Although he acknowledges that *Brady* case law must inform the analysis of the United States' discovery obligations, the defendant devotes ample attention to a Tenth Circuit decision that does not address *Brady* or discovery obligations at all. *See* Def.'s Supp. Br. At 20 (summarizing *Ackerman*'s holding "that the National Center for Missing and Exploited Children (NCMEC) was a government agent *for Fourth Amendment purposes*") (emphasis added). Moreover, the defendant necessarily concedes that discovery obligations under *Brady* and, by extension, Rule 16 are case specific. *See* Def.'s Supp. Br. at 20 ("The critical point is to make an agency determination based on the facts of the particular case. It is not sufficient, for example, to infer an agency-principal relationship based on the structure of government agencies."). The rationale he advances, however, is not focused on the particulars of this prosecution. The defendant's reliance on the inapplicable standard of *Ackerman* highlights these errors.

Start with what the Tenth Circuit did in *Ackerman*—a decision addressing the private

search doctrine. First, in answering the question of whether an NCMEC warrantless search could be considered a government-sponsored search, the Tenth Circuit considered whether NCMEC was a governmental entity *as general matter*—that is, whether "NCMEC's law enforcement powers extend[ed] well beyond those enjoyed by private citizens," "the level of governmental control over [NCMEC], the broad statutory mandates to which it was subject, its dependence on federal funding, the purpose behind its creation, and the benefits it conferred on the government." *Ackerman*, 831 F.3d at 1296–97.

After concluding that NCMEC's general features showed it was indeed a governmental entity, the court then considered the agency relationship between NCMEC and the government *generally*. To determine whether that relationship implicated Fourth Amendment obligations on NCMEC, the Tenth Circuit in *Ackerman* considered a two-part test: (1) whether the government "knew of and acquiesced in" NCMEC's putative search; and (2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends. *See id.* at 1301–02. At the first step, the court relied on "congressional knowledge" of NCMEC's doings. *Id.* at 1302. The second step, too, turned on congressional oversight, looking to Congress's "authoriz[ation] and fund[ing] of NCMEC to perform the functions it performed" and, in turn, NCMEC "undertak[ing] the sort of conduct challenged here precisely because (at least in part) it intends to aid law enforcement." *Id.* Under the final analysis, therefore, NCMEC was deemed part of the government for purposes of the Fourth Amendment.

Here, the defendant cites *Ackerman* after noting that "courts have found third parties to be a part of the prosecution team where they serve as the government's agents in particular cases." *See* Def.'s Supp. Br. at 20. But *Ackerman* is not about "prosecution team" membership as that term is understood in the context of discovery obligations. Instead, the decision focuses

on whether an unlawful, warrantless search by a private actor can effectively be deemed a warrantless governmental search. That issue is not relevant here, where Google responded to a lawfully issued search warrant. That distinction fatally undermines the defendant's fealty to *Ackerman*, a decision premised on the *absence* of a warrant.

2. Attempting to Apply *Ackerman* to the facts of this case demonstrates the inapplicability of the private search doctrine to the scope of the prosecution team under *Brady*.

The inapplicability of *Ackerman*'s standard is made clear from attempting to apply it to these facts. As a general matter, the defendant does not and cannot argue that Google is an actual governmental entity in the normal course of the company's operations. Still, he argues that Google's actions are comparable to NCMEC's in *Ackerman* because "Google had a statutory requirement to assist the government." Def.'s Supp. Br. at 21. Never mind that the statutory commands cited by the defendant focus on service providers' obligations to keep private certain customer information except in limited circumstances, including the issuance of a search warrant. *See* Va. Code § 19.2-70.3(A)(2); 18 U.S.C. § 2703(c)(1)(A). The "statutory requirement" argument falls away with the defendant's concession that "mere compliance with a warrant does not transform its recipient into a government agent." Def.'s Supp. Br. at 22.

Reliance on the two-factor analysis applied in *Ackerman* does not change the calculus. The first factor—government acquiescence in the search—simply makes no sense when applied to these facts. The United States served a search warrant supported by probable cause upon Google. Accordingly, the United States necessarily knew that legal process compelled Google's compliance. As to the second factor—the private party's intent to assist law enforcement—Google's "intent" was irrelevant in the face of compulsory legal process. The warrant mandated the company's efforts. The defendant's argument thus distills to an untenable conclusion: that

mere compliance with a search warrant directs prosecution team analysis. That argument is wrong and should be rejected.

Finally, if this Court were to engage the defendant's reliance on Fourth Amendment agency cases, the Fourth Circuit's decision in *United States v. Richardson* would guide the analysis. 607 F.3d 357 (4th Cir. 2010). In *Richardson*, the court assessed whether AOL acted as an agent of the government when conducting a purportedly unconstitutional search of that defendant's email account, locating pornographic pictures therein, and forwarding those pictures to law enforcement as statutorily required. *See id.* at 363–64. The court analyzed the case using the same factors the Tenth Circuit looked at in *Ackerman*: (1) whether the Government knew of and acquiesced in the private search; and (2) whether the private individual intended to assist law enforcement or had some other independent motivation.

The Fourth Circuit held that there was no government acquiescence or intent to assist by AOL. The court reached that conclusion while noting that AOL's involvement in the investigation resulted from law enforcement's use of "the ordinary forms of compulsory legal process,' i.e., 'two administrative subpoenas and a preservation request' served pursuant to the Stored Communications Act 'for the purpose of identifying the name, address, and other subscriber identifying information for an AOL client.'" *Richardson*, 607 F.3d at 365. The use of compulsory legal process to ascertain information did not compel the conclusion that law enforcement participated in the search or investigation by AOL nor did AOL's return of this information support that AOL "intended to assist the Government in its case." *Id.* When turning to the reporting requirements mandated by statute, the *Richardson* court noted that the requirement did not show an agency relationship because it did not direct AOL to undertake investigatory practices such as "actively seek[ing] evidence of child pornography in certain

circumstances nor prescribed the procedures for doing so in the event that AOL decided to ferret out subscribers using its system to transmit illegal digital images." *Id.* at 366.

Richardson undermines the defendant's position. The Fourth Circuit rejected the kind of statutory reliance touted by the defendant. Nor do the laws here compel Google to monitor users' location information or maintain that location information for law enforcement purposes. Rather, that is the Google user's decision to permit Google to monitor and maintain that location information as well as Google's willingness to store that information that makes it accessible for federal law enforcement. And even with that accessibility, the United States only received the material as a result of a search warrant.

At bottom, the Court should not resort to these Fourth Amendment agency cases when analyzing discovery obligations related to prosecution team membership. But, if the Court does engage this argument, Google remains an independent actor providing a narrow subset of its business records as directed by a search warrant.

3. Google providing a narrowly limited set of business records as compelled by a search warrant does not constitute pre-charge investigation on behalf of the United States in this case.

The defendant argues that there is more than Google's mere compliance in this case that requires they be deemed a member of the prosecution team—they truly investigated the case he urges. The facts of this case reveal, however, that Google did not investigate this case or do anything to further the investigation separate and apart from providing a narrowly limited set of business records in response to a search warrant.

Indeed, the purported investigation to further law enforcement purposes by Google offered up by the defendant is comprised of Google searching its file for business records responsive to the search warrant, engaging with law enforcement as general matter about the

contours of GeoFence warrants, and rebuffing the United States at the second stage of the warrant. These actions by Google are not investigatory in nature.

Google's search for a limited set of business records in this case was necessitated by a search warrant issued by a Virginia magistrate. Further, *every* company has to search its files for material responsive to a search warrant. Service providers commonly review large sets of customer records to produce information in response to appropriately limited legal process. For example, in the traditional telephone context, investigators use subpoenas to identify the people who placed calls to a specified telephone number. A phone company responding to this sort of subpoena, however, may review call records for all of its customers to find this information. Stated simply, the manner of Google's internal practices for complying with compulsory legal process should not factor into the prosecution team analysis.

Yet another example of the boundless rule the defendant endorses is his rationale that Google's involvement with crafting the search warrant as a general matter requires a finding that they are a member of the prosecution team.[2] This contention is entirely untethered to the particulars of this case. There is simply no factual support for the premise that Google advised the lead case agent in the course of securing the search warrant in this case. More to the point of the boundlessness of this rule, technology companies like Google regularly engage in discussions

[2] First Google is responsible for creating the three-step process. *See* Def. Supp. Br. at 22 ("[T]he government obtained a warrant using a tiered disclosure process that Google itself designed."). And, then CellHawk created the search warrant. *See* Def.'s Supp. Br. at 18 ("The defense strongly suspects that the warrant in this case was produced using a template provided by a private company, namely 'CellHawk.'"). The incongruity of these statements make plain the contortions this defendant must undertake to make his case. Google's involvement in the preparation of GeoFence search warrants is not probative of their membership on the prosecution team in this case. Even the defendant concedes that prosecution team analysis looks to the facts of a particular prosecution not of the entities engagement with each other as a general matter.

with law enforcement about the contours of search warrants. These discussions often focus on technological, proprietary, or privacy concerns stemming from language or requests in the warrant.

Lastly, the defendant is incorrect about Google's role at the second stage of the request to demonstrate Google's investigatory role. Google did not determine when the list of users had been sufficiently narrowed. The defendant calls on this Court to disregard common sense. Rather than return the entirety of the additional location information requested at stage two of the search warrant, Google argued in a follow-up phone call to second-stage emails that Google would only provide additional location information at stage two for nine anonymized accounts. By protecting its own interests, which ran contrary to the United States' interest in investigating the robbery, Google asserted control over its own information. The lead case agent accepted Google's proposal due to the time-sensitive nature of identifying the armed robber and his prioritization of obtaining information concerning the defendant's account.

4. The *Brady* prosecution team precedent cited by the defendant demonstrates that Google is not a member of the prosecution team in this case.

When circling back to case law addressing *Brady* prosecution team principles, the defendant again points this Court to cases that demonstrate the futility of his argument. *McCormick v. Parker*, 821 F.3d 1240, 1247 (10th Cir. 2016), *Bracamontes v. Superior Court of San Diego Cty.*, 255 Cal. Rptr. 3d 53, 64 (Cal. Ct. App. 2019), and *United States v. Rosenschein*, No. 16-4571 JCH, 2019 WL 2298810 (D.N.M. May 30, 2019), are cases involving investigatory steps taken by the purported prosecution team member.

McCormick addresses a testifying sexual assault nurse examiner who examined the victim in a sexual assault prosecution to physically corroborate sexual abuse allegations. 821 F.3d at 1247–48. Adopting reasoning from a state court in California, the *McCormick* panel

noted that a "major purpose of the [sexual assault nurse examiner's] examination was to determine whether the allegation could be corroborated with physical findings." *Id.* at 1247. Importantly, the panel made clear that the holding was limited to the facts before it and did not extend, for example, to "an expert who had no pre-charge investigatory role." *Id.* In addition, mere treatment of a sexual assault victim would not suffice. *See id.*

Bracamontes similarly involved a California state court's analysis of a crime laboratory engaged by prosecutors to investigate the defendant's DNA tie to a murder scene. Recognizing that "government crime laboratories" are indisputably members of a prosecution team in cases in which they provide DNA services, the *Bracamontes* court simply concluded that a private criminal lab performing the same duties as part of a contractual obligation with state prosecutors would be treated the same. *See Bracamontes*, 255 Cal. Rptr. 3d at 64–65. As the state court in *Bracamontes* explained of the lab's role, "[t]hey were contracted by the government to conduct DNA testing of critical evidence in an effort to identify or exclude suspects, including [the defendant]." *Id.* at 64.

In *Rosenschein*, a district court in New Mexico analyzed whether NCMEC was a member of the prosecution team. After discussing the *Ackerman* decision, the district court agreed with the United States that Ackerman's analysis "d[id] not necessarily mean" that NCMEC was "part of the prosecution team for discovery purposes." *Rosenschein*, 2019 WL 2298810 at *6; *see also United States v. Nosal*, No. CR–08–0237 EMC, 2013 WL 1352244, at *2 (N.D. Cal. Apr. 3, 2013). Nevertheless, the district court held NCMEC was a member of the prosecution team in that case because the organization NCMEC "did conduct, as it is charged to do by statute, a limited investigation into the facts of this case," "by identify[ing] the location of the suspected internet user through the IP address provided in the CyberTipline reports, and then providing that

information, along with the CyberTipline report(s), to the New Mexico Attorney General's Office." *Id.* at *7. Moreover, "after law enforcement obtained electronic materials from [the defendant's] home, [the officer] sent those files to NCMEC for analysis in order to obtain more information to aid in his investigation." *Id.* at *8.

Each of these cases demonstrates several unifying points that justify denying the defendant's motion: (1) prosecution team analysis focuses on an entity's involvement in a particular case; and (2) the entity or individual undertakes meaningful investigation going to the heart of the case that is not compelled by legal process. The investigatory steps identified in *United States v. Stewart* remain a good guidepost. 433 F.3d 273, 298–99 (2d Cir. 2006) (noting that pre-charge investigation includes interviewing witnesses, gathering facts, or developing prosecutorial strategy). In each of the foregoing cases proffered by the defendant, no legal process was needed to have the entities undertake their work. And their work, to be clear, was sought to conduct actual investigation—examination of a sexual abuse victim in *McCormick*, DNA testing of evidence in a murder investigation in *Bracamontes*, and analysis of files by NCMEC to further the officer's investigation in *Rosenschein*.

In this case, as provided in the United States' supplemental brief, Google is at most a prototypical third-party witness in a criminal case. It possesses information, specifically business documents, relevant to the investigation of a crime, so agents used judicial process to communicate with and compel the production of that information. But participation as a witness—even a cooperative one—does not make one a member of the prosecution team. No different with a business organization cooperating with a federal investigation for its own reasons. Google's involvement in this case is a far-cry from the third-party accounting firm in *Stein* for which prosecutors had a legal right to obtain that party's documents on demand. *United*

States v. Stein, 488 F. Supp. 2d 350, 363–64 (S.D.N.Y. 2007). The United States' right to obtain documents are cabined to the four corners of the search warrant in this case.

As evidenced by the *Brady* prosecution team precedent advanced by the defendant, Google is not a member of the prosecution team in this case.

B. The Defendant's remaining discovery requests should be rejected because he fails to show their materiality under *Brady* and Rule 16.

The defendant calls on this Court to hold that the GeoFence warrant obtained in this case is a general warrant. This Court should therefore focus its analysis on whether the information sought by the defendant is material to whether the GeoFence warrant is a general warrant. When viewed through this lens, the defendant fails to meet his burden.

The defendant's materiality argument splits the documents into two buckets—those that he argues are material under *Brady* and thus, Rule 16 as well, and those that he argues are material under Rule 16 alone. He contends that Requests 1 (Wi-Fi access points), 3 (Google location information collection, analysis, sorting, and accuracy), 4-a, b, e (Details on number of Google users information is collected, deletion of that information, and privacy policies for location information database), and 9 (data initially determined responsive to the warrant, but ultimately excluded) are *Brady* material as they relate to at least one of three issues that are central to the success of his suppression motion: overbreadth, lack of particularity, and lack of voluntariness. *See* Def.'s Supp. Br. at 8. He argues that the remainder of the requests—4(c), 4(d), 5, 11(d), and 12—are discoverable under Rule 16. *See* Def.'s Supp. Br. at 25.

1. The defendant fails to demonstrate that his requests collectively establish *Brady* materiality.

Brady materiality sets forth a "reasonable probability" standard that asks whether, in the context of all the information "collectively, not item by item," "the result of the proceeding would have been different" had the information been disclosed. *Kyles v. Whitley*, 514 U.S. 419,

433 (1995). "The mere possibility that an item of undisclosed information might have helped the defense, or might have affected the outcome of the trial, does not establish 'materiality' in the constitutional sense." *United States v. Agurs*, 427 U.S. 97, 109–10 (1976).

The gravamen of the defendant's materiality arguments is the purported violation of others' reasonable expectation of privacy. The outcome of the suppression motion would not be placed "in such a different light as to undermine confidence in the [outcome]" should the Court deny the defendant's requests.

a. The defendant's materiality argument for Wi-Fi access improperly relies on the location coordinates belonging to others.

The defendant's explication of the materiality surrounding the Wi-Fi access points is premised on three principal contentions: (1) through general understanding of Wi-Fi access points, Google possibly included users in the initial warrant return who were never inside the GeoFence at all; (2) "Mr. Green"—the user whose anonymous identifier ends with 1516—was probably never inside the GeoFence, but was simply driving down a road next to the Journey Christian Church on his way home from a nearby hospital; and (3) disclosure of Wi-Fi access points will permit the defendant to determine how many devices Google may have falsely placed within the 150-meter GeoFence. *See* Def.'s Supp. Br. at 8–9.

As an initial matter, the defendant's argument for the materiality of the Wi-Fi access points fails because it concerns possible Fourth Amendment interests of third parties, not the defendant. It is undisputed that the defendant's expert did not plot for the Court the locations

associated with the anonymous identifier belonging to the defendant.[3] This decision was never explained, however, despite the defendant's expert acknowledging that he had indeed plotted the points related to that account. *See* Disc. Hr'g Tr. at 115–16. And that account was the first-listed account in every single request made by the lead case agent for more information from Google under the search warrant. *See id.*

The defendant does not claim that his phone was not present within the GeoFence during the hour of the bank robbery or that his location information did not in fact fall within the scope of the warrant. His challenge to the warrant therefore fails. It "is black-letter law" that "rather than basing his claim for relief upon the rights of third parties" a defendant must demonstrate that his own rights were infringed. *United States v. Stearn*, 597 F.3d 540, 552 (3d Cir. 2010) (quoting *Rakas v. Illinois*, 439 U.S. 128, 139 (1978)). Indeed, in *Rakas*, the Supreme Court explained that the fundamental question to be answered is "whether the challenged search or seizure violated the Fourth Amendment rights of a criminal defendant who seeks to exclude the evidence obtained during it." *Rakas*, 439 U.S. at 140. The defendant's request for Wi-Fi access points is not material to the suppression of evidence obtained from his Google account.

The defendant's argument for the materiality of the location of Wi-Fi access points suffers from other deficiencies. He fails to explain how he could extrapolate from the location of particular Wi-Fi access points to Google's customer location information, which is derived from

---

[3] Defense counsel only recently acknowledged that they received the defendant's anonymous identifier in their supplemental brief. In all of its filings, however, the United States made plain the location attributes associated with the "Chatrie Account." Moreover, the United States' surreply set forth the final four digits of the defendant's anonymous identifier. *See* United States Surreply at 2, ECF No. 64 ("As to the defendant's anonymous identifier, the defendant has received that information. Specifically, the defendant's identifier is provided in the Google GeoFence returns and ends with 5659."). That disclosure came twenty-two days prior to the discovery hearing in this case.

multiple access points seen by a device at a particular time. And he fails to demonstrate that the fact that cell phone location information inherently has some degree of uncertainty would convert the warrant into a general warrant. The warrant was sufficiently particular because where Google had determined that a device fell within the specified GeoFence, the warrant required Google to disclose its location information.

b. The defendant's fails to demonstrate the materiality of his request for information about Google's collection, analysis, and sorting of location information.

Request 3 similarly does nothing to meaningfully change the Court's analysis of the suppression issue in this case. The defendant has failed to establish the materiality for the request for information surrounding how Google captures and collects location information from users, policies and procedures for collection, storage, and analysis of location information, and the algorithms involved in the collection, storage, analysis, and sorting process.

The defendant's argument for materiality again raises three primary arguments: (1) whether Google actually restricted their search to information voluntarily disclosed is relevant to discretion provided to Google under the warrant;[4] (2) the requests will help confirm the defendant's suspicion that there is a lack of anonymity in the identifiers given to Google users; and (3) Mr. Green's account shows that the accuracy of the location data provided by Google will reveal broader issues of passersby being caught in the first round of the GeoFence warrant. *See* Def.'s Supp. Br. at 9–12.

[4] The defendant's contention that "Google Location Services and Web & App Activity are enabled by default" is unsupported. The defendant's expert's own testimony demonstrated that a Google user would have to approve of Google's collection of information via these services when setting up the Google account.

Google's internal data collection policies and the manner of Google's compliance with the GeoFence warrant in this case are not relevant to the defendant's claim that the GeoFence warrant was a general warrant. The warrant specified with particularity the location information it sought, and if Google failed to fully search its databases to find responsive information, Google's failure would not establish that the warrant was a general warrant. And if Google stores other databases of information not voluntarily disclosed by customers to Google, as the defendant apparently speculates, it would not change the fact that the information Location History information actually disclosed to the government here was voluntarily disclosed. Google's search of their databases and how they maintain these databases cannot convert the warrant into a general warrant.

Similarly, the defendant's contention about anonymity does not establish the materiality of his request. The identifiers ascribed to each Google account in this case kept both the United States and the defendant's expert from identifying them. *See* Disc. Hr'g Tr. at 111–12. Nevertheless, the search warrant sought Google location information, specifically "location coordinates and the data source that this information came from if available." *See* GeoFence Warrant at 4, ECF No. 54-1. That request is made plain in the search warrant. The defendant seems to infer that anonymity of the account identifiers means that the location information will not be useful in solving the crime. Of course, the search warrant indicates that it will be useful—that there is probable cause that location information is evidence of the crime.

Lastly, the defendant bases his argument surrounding the accuracy of information in stage one of the warrant on the account of "Mr. Green" with no mention of coordinates relating to the defendant's Google account. That argument, premised on the location coordinates of another account holder, does not affect this Court's impending decision about purported

violations of the defendant's constitutional rights.

c. The defendant's request for information purportedly bearing on voluntariness is not material to the suppression motion.

The defendant requests information about the total number of users whose information is collected by Google, the retention of user data, and privacy policies relating to the storage of location information as *Brady* material because they bear on the question of voluntariness. *See* Request 4 subparts (a), (b), and (e).

Although the number of Google users whose information is collected by Google may inform the Court's understanding of Google's prowess as a corporation, that number of users does not inform whether the warrant in this case is a general warrant or whether the defendant had a reasonable expectation of privacy in Google location information. The number of Google users whose location information is collected by Google also does not bear on voluntariness. The number of customers held by the bank in *United States v. Miller*, 425 U.S. 435 (1976), or the number of consumers using the telephone company in *Smith v. Maryland*, 442 U.S. 735 (1979), did not inform the Court's analysis.

Neither did the raw numbers of users having cellphones decide the question of voluntariness in *Carpenter v. United States*, 138 S. Ct. 2206 (2018). In *Carpenter*, the Supreme Court concluded that a "chronicle of a person's physical presence compiled every day, every moment, over several years" "without any affirmative act on the part of the user beyond powering up" did not implicate the third-party doctrine. *See Carpenter*, 138 S. Ct. at 2220. The facts in this case surrounding voluntary disclosure are straightforward—the defendant, by his own expert's admission, voluntarily disclosed the two hours of location information sought in this case. *See* Disc. Hr'g Tr. at 107. Google's storage of the defendant's location information took far more than him powering up his cell phone: he had to affirmatively opt in multiple times

to enable Google's collection and storage of his Location History information. *See* Google Amicus Br., ECF No. 59-1 at 8. Moreover, the request for retention disregards that it is the user who controls Google's retention of the data. Google confirmed that even after the defendant chose to have Google store his location information, he retained the ability to delete it: "[t]he user can review, edit, or delete her Timeline and [Location History] information from Google's servers at will." *Id.* at 8.

Lastly, as provided in the United States' supplemental brief, Google's privacy policy is publicly available. The notion that additional discovery is required because Google does not reference "Sensorvault" skips over the fact that the term does not appear to be in Google's lexicon. The relevant information is publicly available.

d. The defendant's request for location information initially determined to be responsive by Google, but excluded from final production to law enforcement improperly focuses this Court's attention on Google's internal processes.

The defendant seeks information not provided to law enforcement because, he argues, this non-responsive information would demonstrate "that the pool of users subject to search by Google was larger than Google has acknowledged, supporting Mr. Chatrie's overbreadth and particularity arguments." Def.'s Supp. Br. at 17. The defendant's argument here fails to demonstrate materiality. At bottom, the defendant's argument is simply a recitation of the contention that Google's manner of responding to the search warrant informs the constitutionality of the GeoFence warrant. But the warrant specified its objects with particularity, and if Google failed to produce responsive information, Google's failure would not transform the warrant into a general warrant. Similarly, whether Google searched across many users does not change make the warrant a general warrant. Service providers commonly review large sets of customer records to produce information in response to appropriately limited legal

process, such as where Google is required to disclose identity information for subscribers who accessed their Google accounts from a specified IP address during a particular time period. The United States does not dispute that a vast number of people have Google accounts: that fact follows from the facts set forth in the search warrant affidavit. The Court's analysis of the constitutionality of the GeoFence warrant in this case needs no further clarification on Google's manner of compliance.

2. The defendant also fails to establish that his remaining requests significantly alter the quantum of evidence in his favor.

The defendant argues that the remainder of his requests—4(c), 4(d), 5—are discoverable under Rule 16. *See* Def.'s Supp. Br. at 25-26. The defendant, however, fails to meet his burden of advancing facts that indicate any of these requests will actually prove his suppression defense. None of the requests speak to any of the issues critical to the Court's suppression analysis. Accordingly, the Court should reject the requests.

In request 4(c), the defendant seeks a list of who has access to the location information database because he contends that it will aid the defense in identifying witnesses with knowledge of the Sensorvault and its operations. The request in 4(d) seeks disclosure of how Google maintains the database because, he argues, this information will reveal what data goes into the "Sensorvault, how it is stored, and when, if ever, Google deletes it." Def.'s Supp. Br. at 26. Lastly, in request 5, he calls for the names and qualifications of the individuals from Google involved in the GeoFence warrant process.

Under Rule 16, the defendant bears the burden to demonstrate that the requested discovery will enable him to "significantly alter the quantum of proof in his favor"—not just that the information bears some abstract logical relationship to the case. *Caro*, 597 F.3d at 621. To meet that burden, he must provide "facts . . . indicating that the information would . . . actually

help[ ] prove his defense." *Id.* As stated in *United States v. Mandel*, a decision cited approvingly in *Caro*, "[n]either a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense." 914 F.2d 1215, 1219 (9th Cir. 1990). In *United States v. Armstrong*, the Supreme Court explained that, under Rule 16, "'the defendant's defense' means the defendant's response to the Government's case in chief." 517 U.S. 456, 462 (1996).

The bottom-line inquiry for the Court should be whether the defendant put forth "facts" that the requested discovery would "actually help[ ] prove his [suppression] defense." *Caro*, 597 F.3d at 621.

a. The defendant's request for who at Google has access to the location information database, how that database is maintained, and names of individuals involved in the GeoFence process are not material under Rule 16.

The defendant fails to appreciate that Rule 16 materiality analysis calls for more than mere helpfulness—there must be "a strong indication that [the requested materials] will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal." *Caro*, 597 F.3d at 621. This "strong indication of an important role" requirement must be understood through the prism of the overarching principle that materiality be premised upon facts showing that the materials will actually help prove a defense. The defendant fails to meet his burden.

Neither who maintains the location information database for Google or the type of information in that database touches on the broader questions guiding suppression in this case—whether the defendant had a reasonable expectation of privacy in two hours of Google location information and whether the GeoFence warrant is a general warrant. These requests will not

speak to the defendant's voluntary opt-in or whether the warrant is a general warrant. By the same token, the retention of location data is similarly unavailing for the defendant for the reasons discussed earlier. As stated earlier, it is the user who controls Google's retention of the data. Google confirms that even after the defendant chose to have Google store his location information, he retained the ability to delete it: "[t]he user can review, edit, or delete her Timeline and [Location History] information from Google's servers at will." ECF No. 59-1 at 8.

As to his request for names and certification of Google analysts involved in the GeoFence process in this case, the defendant has been provided with the email address, business address, and names of the Google employees who have supplied the information to the United States pursuant to these search warrants. The continual prodding for this information simply makes little sense and demonstrates a plain lack of due diligence on behalf of the defendant. The Court should not burden the United States with offering more than what has already been provided.

C. The Defendant Narrowing Process and other Law Enforcement Focused Requests

The Court's supplemental briefing Order directed the parties to address materiality and obligation to obtain information from Google. Because the United States understood the Court's order to be focused on Google documents, it did not address requests 8 and 11 in the initial round of supplemental briefing.

1. Disclosure of the Narrowing Process used by the Lead Case Agent.[5]

At the hearing on January 21, 2020, the United States made abundantly clear that no discoverable material existed on the narrowing process that had not been disclosed.

[5] The defendant's request 10 for names, training, certification, and qualification of law enforcement analysts should be denied as moot. The defendant has received the *curriculum vitae* of Special Agent Jeremy D'Errico who will serve as an expert in this case. The lead case agent does not have a *curriculum vitae* and will not be called on to offer expert testimony. Should either fact change, the United States will update opposing counsel.

Nevertheless, the United States agrees with the Court's assessment that practically giving some insight prior to the suppression hearing of the narrowing process will facilitate a more streamlined suppression hearing. To permit preparation for the hearing, the United States advised lead defense counsel that she and her team would be provided with a summation of the lead case agent's rationale for culling from nineteen anonymized accounts to nine anonymized accounts and then the reasoning for selecting the final three accounts.

At stage one, the lead case agent applied a general rule that any device associated with an account present within the GeoFence radius two minutes after the conclusion of the armed robbery could be excluded from Google's return of additional location information in stage two of the search warrant. Only one of the nine devices did not fit this rule.[6]

After receiving stage two returns for each account, the lead case agent sought subscriber information for three accounts under stage three of the GeoFence warrant. One of those accounts belonged to the defendant—the Chatrie Account. The Chatrie Account was of particular interest to the lead case agent because it was associated with a device that: (1) was near the church prior to the robbery at the same time that the church witness recalled seeing the suspicious individual; (2) inside the credit union during the robbery; and (3) immediately left the area following the robbery via the area near the church. The other two devices were of interest as well. One of those devices belonging to the individual the defendant's expert referred to as "Mr. Blue" whose device ended with anonymous identifier 2662. *See* Disc. Hr'g Tr. at 103-04. The lead case

[6] This particular device had only Wi-Fi points in its stage one returns and those points were near the front of Journey Christian Church in the parking lot area. These points were potentially indicative of a conspirator of the armed robber. In addition, of the devices that were outside of the two minute timeframe, this particular device was the closest in time to that two minute time frame.

agent was interested in further assessing that account's connection to the armed robbery given the possibility that the device associated with the account may have been powered off or otherwise inaccessible in an attempt to evade discovery during the crime. The final account included in the stage three returns belonged to a device that had a travel pattern before and after the robbery that was similar to the defendant's.

Again, however, to the extent that the defendant is seeking this Court's approval of a path to suppression premised on the purported privacy rights of others, this Court should flatly reject that invitation. And questions that needlessly take the Court down that road are inappropriate.

2. No documents fit within the ambit of the defendant's request for law enforcement materials.

The materials composing request 11 simply do not exist within the Federal Bureau of Investigation. The Federal Bureau of Investigation agents in this case indicate that such information, particularly training materials and contracts and memorandums relating to Google location information and or the use of GeoFence warrants do not appear to exist. That position remains the same as the United States set forth in its response to the defendant's motion for discovery.

3. The defendant's recasting of his fishing expedition request 12 should be rejected.

Lastly, the defendant attempts to recast his already-overreaching request 12 for "[a]ll records produced as a result of the requests described above," as a request for communications between law enforcement and prosecutors about GeoFence warrants. *See* Def.'s Supp. Br. at 27-28. The Court should reject request 12 as the fishing expedition request that it is. Nevertheless, the United States has reviewed the communications in this case and there are no communications about the GeoFence warrant obtained in this case that implicate *Brady*. In addition, the lead case

agent will make clear that he was never counseled against the constitutionality and or propriety of the GeoFence warrants he obtained prior to this case.

D. Path Forward Following Supplemental Briefing

The United States does not believe further evidence or argument is needed on the discovery issue in this case. Google's counsel indicates that the corporation will provide an affidavit later this week that will address factual assertions made in its Amicus brief, issues related to those factual assertions, and the defendant's discovery requests. Following receipt of that affidavit, one or both parties likely will still seek testimony from a Google representative at the suppression hearing. An early May date for the suppression hearing appears appropriate at this time.

III. CONCLUSION

The Court should deny the defendant's motion to for discovery.

Respectfully submitted,

G. Zachary Terwilliger
United States Attorney

By: /s/
Kenneth R. Simon, Jr.
Peter S. Duffey
Assistant United States Attorneys
United States Attorney's Office
919 E. Main Street, Suite 1900
Richmond, Virginia 23219
Phone: (804) 819-5400
Fax: (804) 819-7417